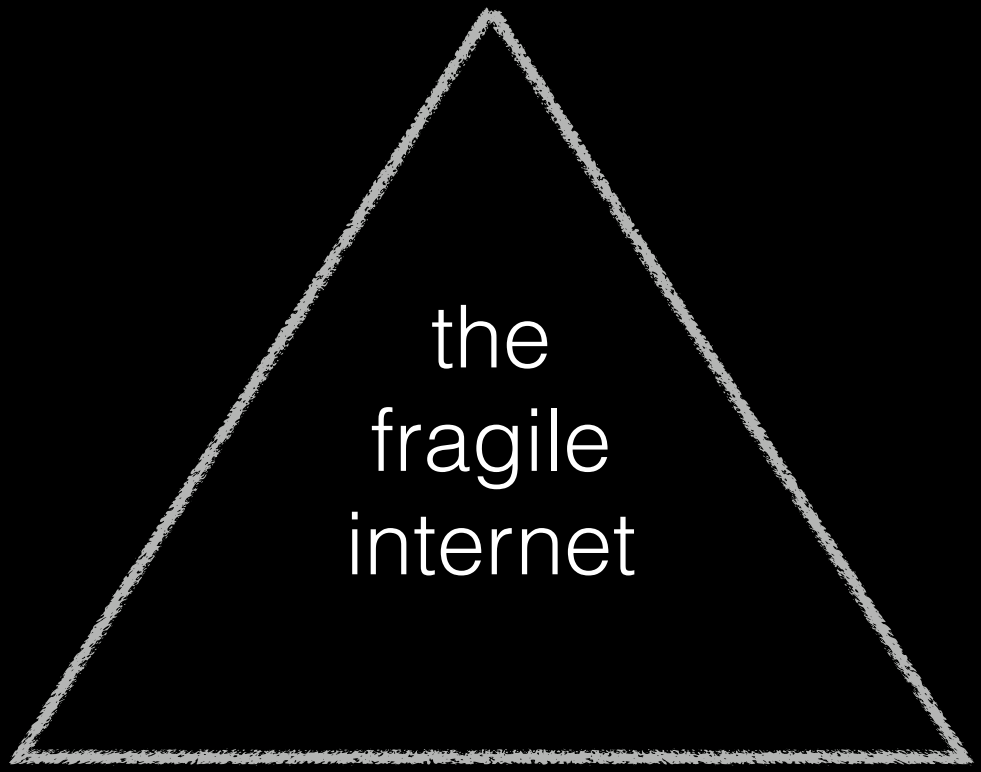
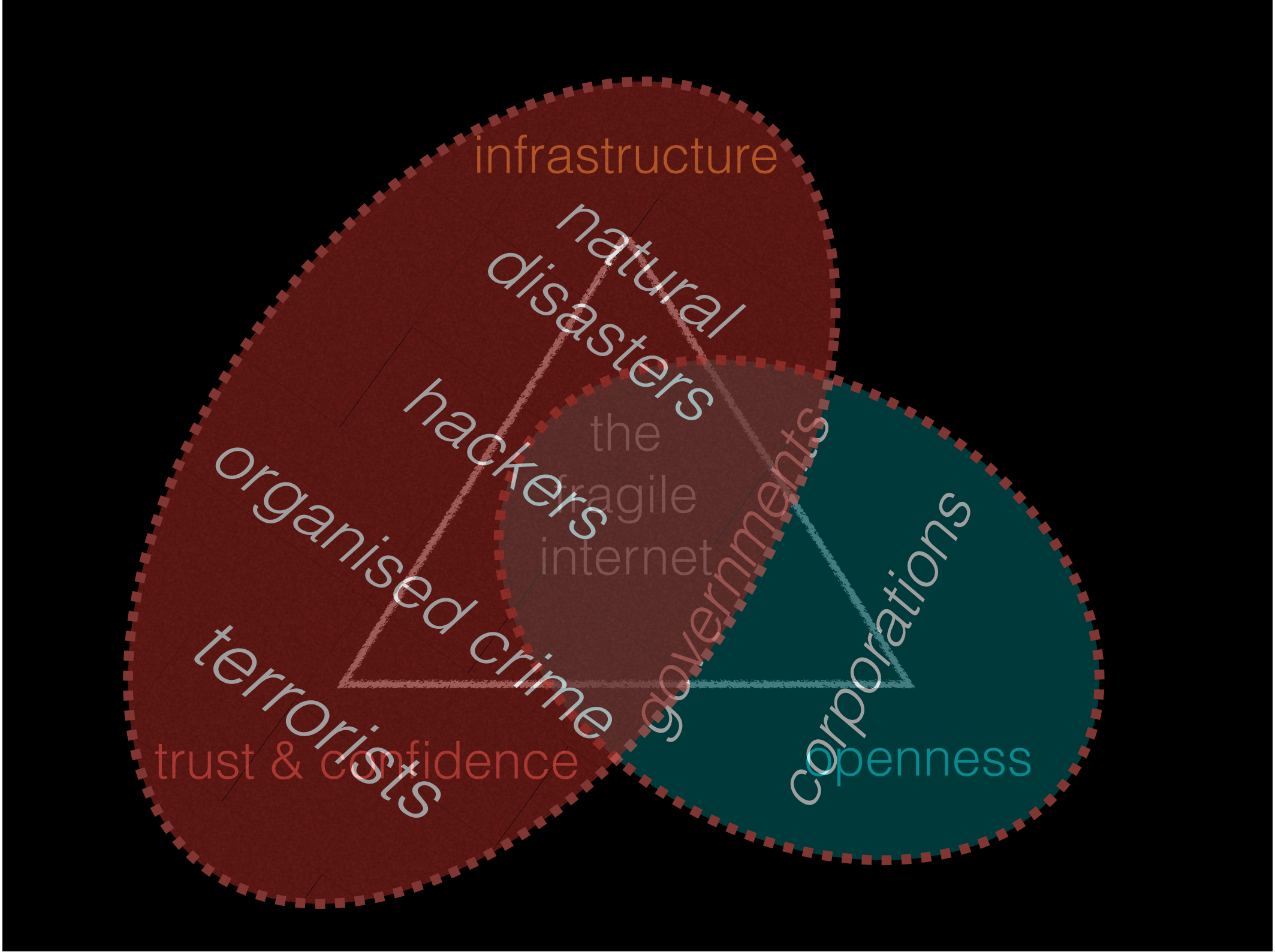
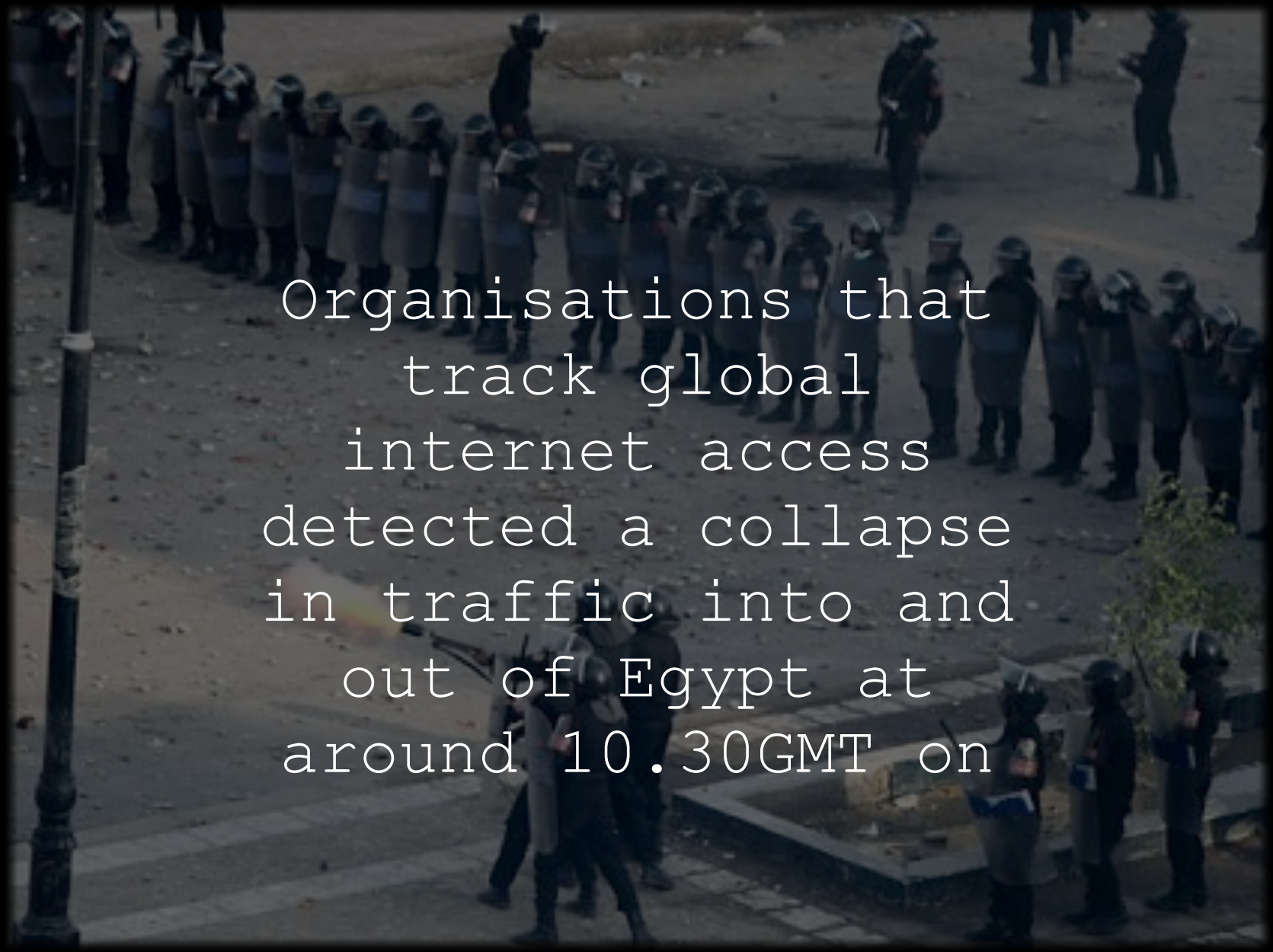
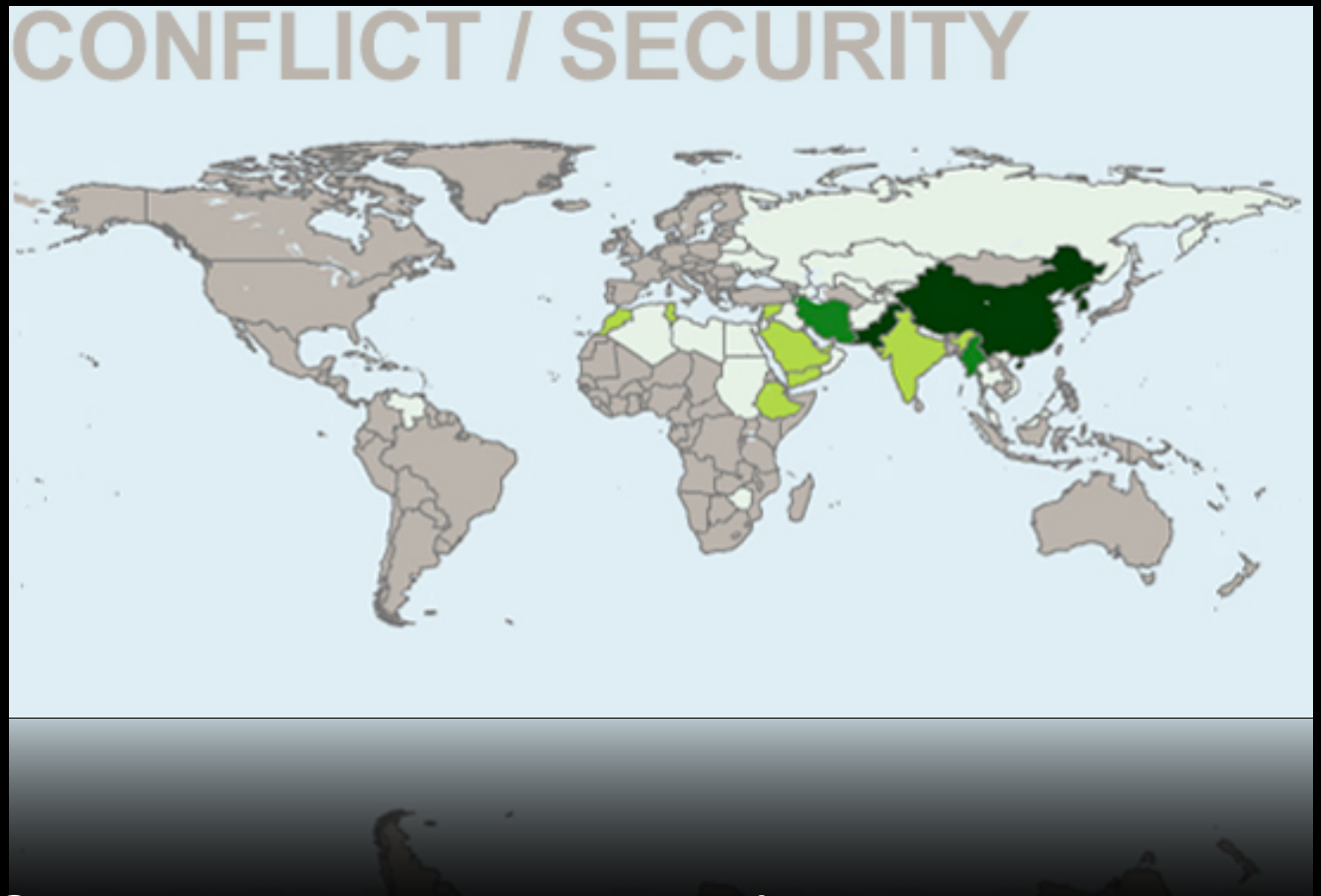

the
fragile
internet


infrastructure
natural disasters
hackers
organised crime
terrorists
trust & confidence
the fragile internet
governments
corporations
openness

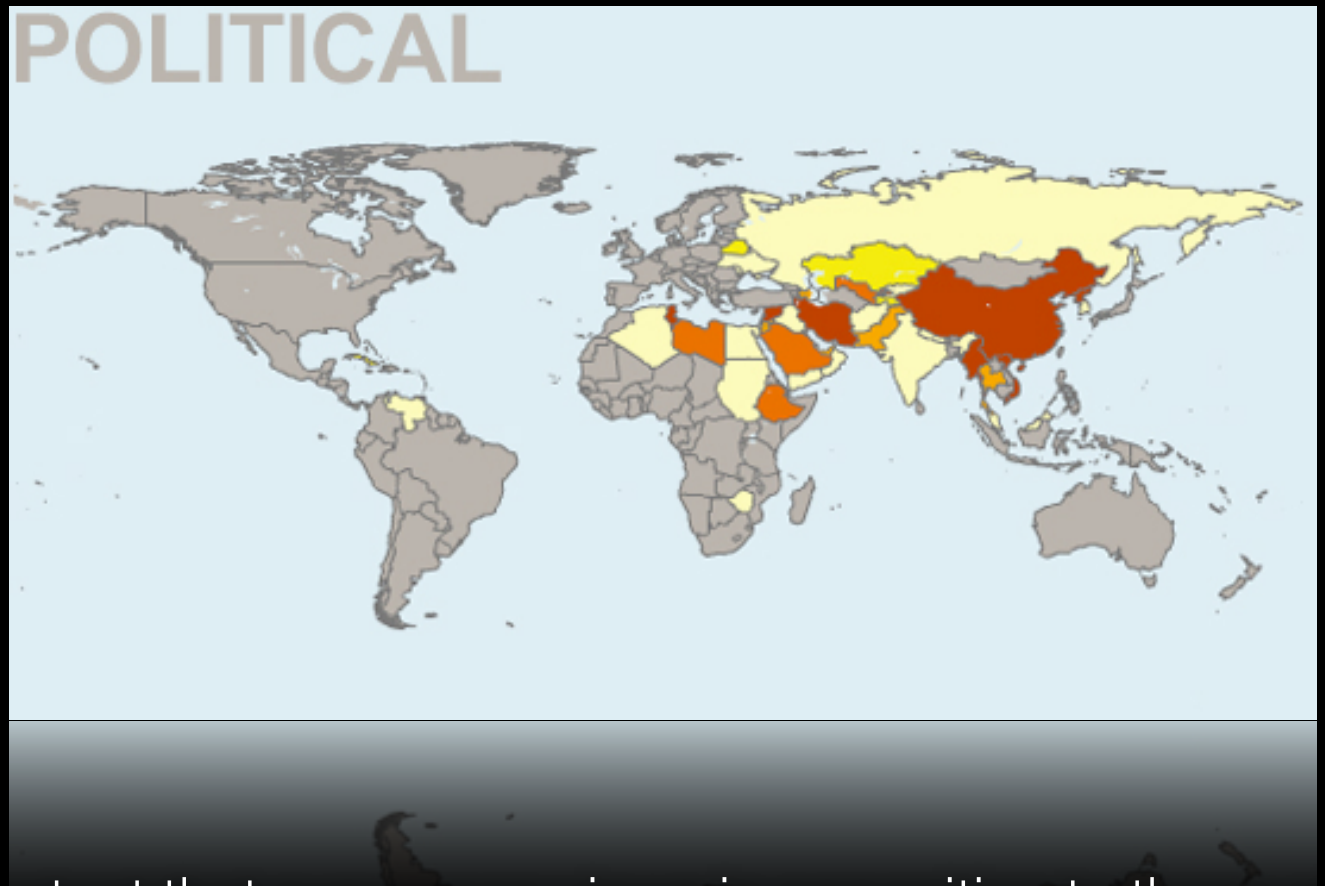
openness


Organisations that
track global
internet access
detected a collapse
in traffic into and
out of Egypt at
around 10.30GMT on

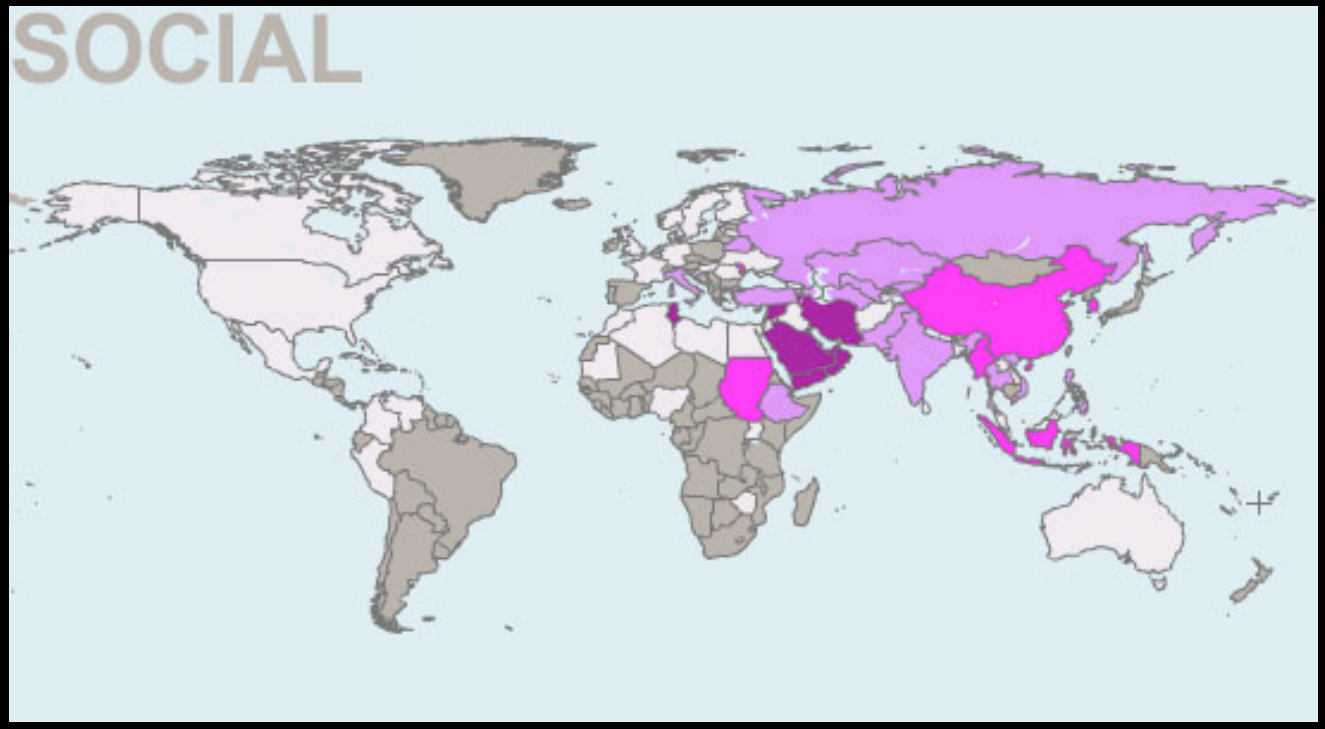

Control Internet?
Yes
No
DELL



Content related to armed conflicts, border disputes, separatist movements, and militant groups.

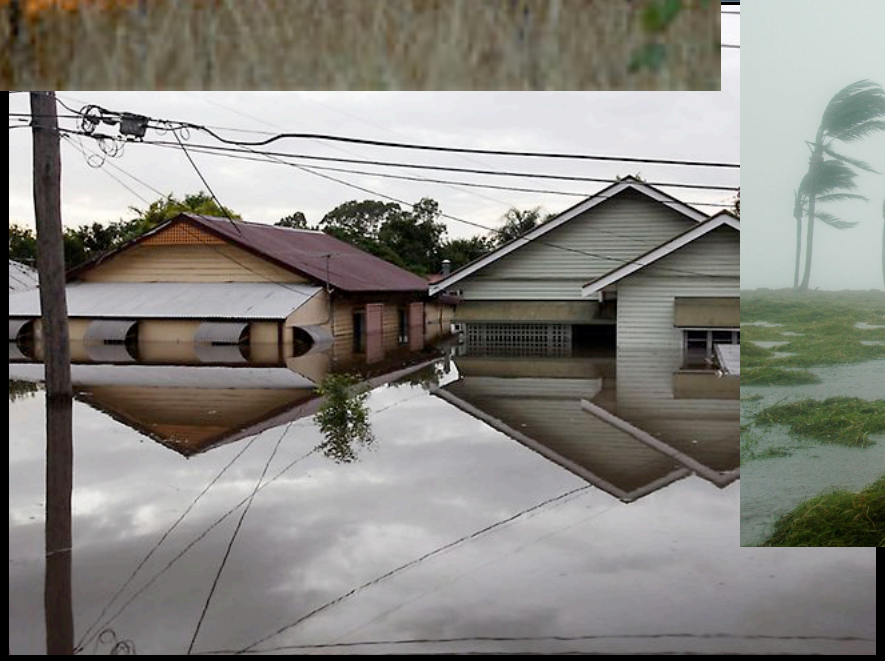


Content that expresses views in opposition to those of the current government, or is related to human rights, freedom of expression, minority rights, and religious movements



Content related to sexuality, gambling, and illegal drugs and alcohol, as well as other topics that may be socially sensitive or perceived as offensive.

infrastructure



trust & confidence


EPIC
FAIL!

- Mariposa botnet
- 12.7m hosts
- 800,000 users details stolen
- empowered relatively unskilled cyber criminals to inflict major damage and financial loss
- persistent and dynamic threat

meanwhile at the enterprise...

- advanced persistent threat
- theft of IP
- game has changed from keeping them out to monitoring and risk management

voluntary code of practice for Australian ISPs to mitigate zombie botnet activity

INTERNET INDUSTRY CODE OF PRACTICE

INTERNET SERVICE PROVIDERS
VOLUNTARY CODE OF PRACTICE

FOR INDUSTRY SELF-REGULATION
IN THE AREA OF CYBER SECURITY

Implementation Version 1.0
1 June 2010

Internet Industry Association
www.iia.net.au

Promoting a safer, fairer, faster, more trusted internet for Australia

Detect

Notify

Escalate

(Report)

Commenced Dec 1, 2010

34 participating ISPs

Representing >90% market coverage

How to Fix Your Infected Computer

icode

Why has my Internet Service Provider directed me to this page?

Australian ISPs are supporting a new national scheme called the icode to help protect their customers and their networks. You may have been directed to this site because your ISP's systems show your computer could have been infected by malicious software (or 'malware') such as a computer virus.

Continue reading this

What is the icode?

On the 1st of December, 2010, the icode commenced. You can read more about the icode on the IIA website. Click here to read the article.

So what can you do?

- Avoiding Infections to get the hottest tips to keep your system more secure.
- Self Help offers ways to detect and remove malware, with links to online resources.
- Professional Help tells you about professional help to deal with an infected computer.
- Sitemap/Search if you would like a one-page overview of what is available on this site or wish to search this site.

Government endorsed

The Internet Industry Association in conjunction with the Australian Government has developed a voluntary code of practice for ISPs. The icode is designed to provide a consistent approach for Australian ISPs to help inform, educate and protect their customers in relation to cyber security risks.

Make sure you use an ISP that is compliant with the icode, look for the Trustmark below on their website.

icode compliant

Next steps

More info www.icode.net.au